Remarks

To facilitate an interview applicant submits this draft response concerning the differences between the claimed invention, particularly claim 1, and the prior art, particularly Hiroya et al. (US 5,754,654) and Rosen (US 5,898,154). The various parts of the Office Action (and other matters, if any) are discussed below under appropriate headings.

Claim Rejections - 35 USC § 102 and § 103

Claims 1, 3-48, 51-53, 61-63, 65-69 and 74 have been rejected under § 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,898,154 to Rosen ("Rosen") in view of U.S. Patent No. 5,754,654 to Hiroya et al. ("Hiroya") and further in view of Schneier's Applied Cryptography, Second Edition ("Schneier").

Regarding claim 1

Claim 1 recites a method of providing a value note comprising the following steps:

> providing first information representative of a bearer's public key information, or from which a bearer's public key information can be verified;
>
> providing second information representative of a commodity represented by the value note; and
>
> calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of an issuer's public key information.

Hiroya et al.

On page 3 of the Office Action dated June 2, 2004, claim 1 was rejected as anticipated by Hiroya because:

> Hiroya et al. teach an electronic ticket vending system such that Applicant's value note reads on the electronic ticket storage device, Applicant's first information reads on PTi, Applicant's second information reads on the ticket information, 610, and Applicant's step of calculating third information (RSA type

signature - asymmetric encryption algorithm) reads on STk and column 15, lines 38-44.

Several aspects of claim 1 related to the first and third information, however, are missing in Hiroya et al. To begin with, the first information of the claimed invention does not read on PTi or any other aspect of Hiroya et al. Even though the first information and PTi are both called public keys, they serve completely different functions within the respective inventions and their similarities end with their names.

Claimed First Information

The first information of the claimed invention represents the bearer's public key information. The bearer's public key is utilized for authentication purposes, specifically, "to verify whether the bearer's signature is correct when the value [note] is redeemed." Specification, page 6, lines 11 and 12. In general, authentication makes sure the value note is provided by the actual bearer who claims to be sending it. Therefore, the public key allows the issuer to verify that a particular value note is being redeemed by the bearer to whom it was issued.

In Hiroya et al., however, PTi is a public key that is utilized for encryption purposes rather than authentication. Encryption also provides security to the system but not in the same way authentication does. Generally, encryption translates data into an undecipherable form in order to ensure data is not read by unauthorized individuals. As explained in Hiroya et al. in columns 16 and 17, PTi is actually used to decrypt the message sent between the electronic ticket storage device and the electronic ticket vending and refunding device. The actual ticket data, transaction identification, and transaction sequence number are included in a message R. R is encrypted by the local secret key before being sent by the electronic ticket storage device. On the receiving side, the electronic ticket vending and refunding device decrypts "the message R using the public key PT12." (PT12 being a specific instance of PTi). Column 17, lines 14 and 15. Therefore, the first information and PTi clearly serve distinctive purposes in their respective systems. The claimed first information is used for authentication while Hiroya et al.'s PTi is used for decryption.

Relationship Between First and Third Information

Another feature present in the claimed invention and lacking in Hiroya et al. is the relationship between the first and third information. This relationship ties together the ability to authenticate a value note and also to ensure that the value note was not

altered. In the claimed invention, the issuer's key is used to "sign" the data of the value note and the issuer's signature represents the third information of claim 1. In Hiroya et al., the secret key, STk, is used to "sign" the ticket information data. Column 15, line 44. The difference is that the first information discussed above is included in the signed information in the claimed invention, while Hiroya et al. fails to disclose data equivalent to the public key of the bearer, i.e. the claimed first information. Consequently, in the claimed invention the bearer's public key is part of the signed information, which ensures that the public key has not been altered since the note has been signed. In Hiroya et al., only the ticket information data is signed. The ticket information data includes "a ticket publication source, an event name, a day and time, a place name, a seat number, and a serial number." Column 15, lines 31-34. Therefore, the signature can only be used to verify that the ticket information data has not been altered and nowhere in the signed information is a public key that is used for authentication purposes.

Schneier

In the Reply to the Office Action dated June 18, 2003, Applicant made reference to Applied Cryptography, 2nd ed., written by Bruce Schneier, to point out that Hiroya et al. reverses the traditional usage of public and private keys. In the Office Action dated June 2, 2004 on page 4, the Examiner responded: "Schneier discloses reversing the traditional procedure of using public and private keys for encryption/decryption as well as using PKI for digital signatures." The reason for referencing Schneier, however, was not to suggest a key could be used for both encryption/decryption and digital signature purposes. The reference meant to show that Hiroya et al. reversed the traditional roles of public and private keys and disclosed them in a rather unconventional and counterintuitive manner. Traditionally, public keys are used for encryption and private keys are used for decryption. (See Applied Cryptography, p. 31.) The reason is because public keys are not kept secret, as suggested by their name. Having a system that allows anyone with a public key to decrypt a message is counterintuitive. Therefore, the traditional method is to encrypt a message with a public key that is widely available, and enable only those with the secret key to decrypt the message.

Hiroya et al. suggests a double encryption method where the secret keys encrypt the message and the public keys decrypt the message. In preparing an electronic ticket for transmittal, for example, the electronic ticket vending and refunding device encrypts a public key, PT12, with a secret key, STg, and encrypts the message, R, with a secret key ST12. Column 17, line 8. On the receiving side, the electronic ticket storage device uses public keys to decrypt the transmitted electronic ticket.

Column 17, lines 12-15. Therefore, an intercepted transmition could be decrypted by anyone with the public keys. In column 16, lines 45 and 46, Hiroya et al. specifically states that each ticket storage device retains the global public key, PTg. Consequently, each ticket storage device could decrypt any electronic ticket. This is why secret keys are traditionally used for decryption, namely, to that ensure only authorized parties with secret keys can decrypt a message.

Consequently, it would not have been obvious to one of ordinary skill in the art at the time of the invention to combine "Hiroya/Rosen/Schneier" as suggested. Office Action dated June 2, 2004, page 4. In contrast, it would be rather surprising for one of ordinary skill in the art to follow such a counterintuitive method of using public and private keys. As a result, the claimed invention does not use the public and private keys similarly to Hiroya et al.

In summary, the third information of the claimed invention includes a signature which signs the first information containing the bearer's public key. The public key is used for authentication and ensures the value note is provided by the actual bearer who claims to be sending it, while the signature ensures that the public key in the first information is not altered. This intertwined relationship between the first information and the third information enhances both authentication and the ability to ensure that the public key has not been altered. Hiroya et al. has no such relationship between an electronic signature and a public key. First, PTi is used for decryption rather than authentication. Second, the electronic signature in Hiroya et al. is only used to sign the ticket information data, rather than any data that could verify the bearer of a ticket. Therefore, claim 1 does not read on Hiroya et al.

Rosen

On page 3 of the Office Action dated June 2, 2004, claim 1 was rejected as anticipated by Rosen because:

> Rosen teaches an electronic monetary system such that Applicant's value note reads on element 11, Applicant's bearer's public key information (first information) reads on identifier for money generator module, element 6, Applicant's information representative of a commodity (second information) reads on the type of note (credit or currency), Applicant's issuer's signature and issuer's public key information reads on the issuing bank's identifier and column 14, lines 6-14, Applicant's redemption instruction reads on column 19, lines 30-65 (Body group of data fields) and Applicant's bearer's signature reads on the

digital signature of the Money Generator module, element 6 and columns 19 and 20, lines 54-67 and lines 1-4, respectively.

Rosen also fails to teach or suggest the relationship contained in the claimed invention between the first and third information. The value note of the claimed invention does not read on element 11 because element 11 does not contain any information that resembles the first information of the claimed invention. The data fields that make up element 11 are listed in column 19, line 34, and none of the data fields resemble a bearer's public key. The bearer's public key information does not read on the identifier for the Money Generator module as stated by the Examiner. The claimed bearer's public key represents the bearer who obtains a value note from the issuer and is used to authenticate the bearer when the note is redeemed or transferred. In Rosen, the Money Generator module "generates the electronic money" and accordingly is the issuer rather than the bearer with respect to the claimed invention. Column 16, lines 62 and 63. Therefore, element 11 does not contain a public key that represents a bearer.

The Transaction money module in Rosen more closely resembles the bearer in the claimed invention. Element 11, however, does not contain any data field that represents a public key of the Transaction money module. Therefore, since element 11 does not contain a data field that resembles the claimed first information it would be impossible to include a signature that signs such information. The signature in Rosen does not sign any information that can be used to authenticate that an electronic note was sent from a particular Transaction money module. Instead, the signature signs identifying information for the Money Generator module which functions as the issuer rather than the bearer. Consequently, Rosen does not utilize the relationship between the first and third information found in claim 1.

Another difference between a value note and element 11 is explained by the way the differing systems are used. For a value note, a feature of the invention allows an issuer to verify whether the note is being redeemed by the correct bearer. This is similar to the way paper checks are used in that a bank needs to ensure a check is tendered by the correct bearer by requiring them to sign the check. Similarly, the bearer's public key is used to authenticate the bearer and the public key is signed by the issuer to ensure it has not been altered. In contrast, Rosen's element 11 is used more like cash rather than a check. The electronic notes can be transferred several times and it is unnecessary for the issuers to verify the original bearer since subsequent bearers can also redeem the electronic notes. In Rosen's system it is important to know that the electronic note was issued by a valid Money Generator module, a valid

issuer. Therefore, Rosen signs the identifying information of the Money Generator module rather than a bearer.

Another difference is that the claimed value notes must be returned to the issuer for each transfer. The bearer's public key in the first information is changed to represent the new bearer before a new value note can be issued. In contrast, since element 11 in Rosen more closely resembles cash, it does not have to be reissued by the Money Generator module each time it is transferred. For a valid transfer of the claimed value note, the claimed first information must be changed to the public key of the new bearer, which is then subsequently signed by the issuer. The reason an electronic note in Rosen does not need to be reissued is due to its lack of a bearer's public key. In summary, the claimed value note contains first information that represents the public key of the original bearer the value note is issued to. This public key is used to authenticate the bearer when a note is redeemed or transferred to a new bearer.

Furthermore, this first information is signed by the issuer to ensure it is not altered. When being transferred, the issuer creates a new value note with new first information that represents the new bearer so that new bearer can be authenticated when they subsequently either redeem or transfer the value note. The public key is signed by the issuer to ensure it remains unaltered and the signature is represented in the third information. In Rosen, element 11 does not contain any field used for authentication of the original bearer. This is because the electronic notes can be transferred "just like paper money" without being reissued and authentication of the original bearer is not important. See Rosen, column 18, line 63.

Rosen does describe electronic credit notes, as opposed to currency notes, that can only be transferred by the owner of the account, similarly to how the claimed value notes can only be transferred from the original bearer. These electronic credit notes, however, still lack data similar to the claimed first information. The account number identifier that identifies the account owner and recipient of an electronic credit note is different from the first information of the claimed invention. Rosen's account number is not in the form of a public key and therefore cannot provide authentication that the actual account holder transferred the electronic credit note. The claimed value note's first information can ensure that the bearer seeking redemption is the actual bearer to whom the value note was issued by using the public key.

Conclusion

In conclusion, the claimed invention utilizes the bearer's public key and the issuer's digital signature in an interlocking manner that provides a very secure method of issuing value notes that is not present in either Hiroya et al. or Rosen. The interlocking manner between the first and third information provides for secure authentication, by the issuer, of the original bearer of a value note, and also provides the ability to ensure that the public key used for authentication, as well as additional information, has not been altered.

In view of the foregoing, request is made for timely issuance of a notice of allowance.

Respectfully submitted,

RENNER, OTTO, BOISSELLE & SKLAR, LLP

DRAFT

By_____
Christopher B. Jacobs, Reg. No. 37,853

1621 Euclid Avenue
Nineteenth Floor
Cleveland, Ohio 44115
(216) 621-1113

Z:\SEC152\152\DWB\DYOU\P\P0185\P0185US.R07.wpd

CERTIFICATE OF MAILING (37 CFR 1.8a)

I hereby certify that this paper (along with any paper or thing referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: _____

_____
Kristine A. Webb